DUMPSARENA

Certificate of Competence in Zero Trust (CCZT)

Cloud Security Alliance CCZT

Version Demo

Total Demo Questions: 8

Total Premium Questions: 80

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

Which of the following is a required concept of single packet

authorizations (SPAs)?

A. An SPA packet must be digitally signed and authenticated.

B. An SPA packet must self-contain all necessary information.

C. An SPA header is encrypted and thus trustworthy.

D. Upon receiving an SPA, a server must respond to establish secureconnectivity.

ANSWER: B

Explanation:

An SPA packet must self-contain all necessary information. Single Packet Authorization is designed to convey an access request in one packet that a receiving enforcement point can validate without first exposing a listening service or initiating a preliminary exchange with the requester. The packet carries the data needed to establish its legitimacy, commonly including such elements as a timestamp, nonce or random value for replay protection, client identity or authorization data, and cryptographic protection. The receiving system evaluates this self-contained request and, only when it validates successfully, can modify access controls to permit the requested protected connection. This model supports Zero Trust principles because the protected service remains undiscoverable and unavailable until a valid, narrowly scoped authorization request has been processed. It also reduces the externally visible attack surface: an invalid SPA packet should not cause the service to reveal information or engage in a session. The Cloud Security Alliance describes SPA as a core capability in Software-Defined Perimeter architectures, where authentication and authorization precede network connectivity. See the Cloud Security Alliance Software-Defined Perimeter Specification and the fwknop Single Packet Authorization documentation.

QUESTION NO: 2

A policy engine authorizes a user to access a confidential document repository. The policy administrator must now enable the approved session. What is the policy administrator's primary role in this transaction?

A. Evaluate contextual inputs and determine whether access is permitted.

B. Collect device telemetry and threat-intelligence information.

C. Establish or terminate the communication path in accordance with the policy decision.

D. Inspect all resource traffic for malicious content.

ANSWER: C

Explanation:

The policy administrator translates the policy engine's decision into operational instructions to establish, modify, or terminate the communication path. The policy engine is the component that makes the authorization decision using policy and contextual inputs. The policy enforcement point applies the resulting controls on the access path to the enterprise resource. Therefore, the policy administrator coordinates the decision's execution rather than independently deciding access or merely collecting telemetry.

QUESTION NO: 3

When planning for a ZTA, a critical product of the gap analysis

process is_____

Select the best answer.

A. a responsible, accountable, consulted, and informed (RACI) chartand communication plan

B. supporting data for the project business case

C. the implementation's requirements

D. a report on impacted identity and access management (IAM)infrastructure

ANSWER: C

Explanation:

The implementation's requirements are a critical product of Zero Trust Architecture gap analysis because the analysis translates the difference between the organization's current security posture and its desired target state into actionable capabilities, specifications, and acceptance criteria. These requirements establish what the implementation must achieve, such as the needed protections for resources, identity and device signals, policy enforcement capabilities, telemetry, integration points, and operational processes. They give architects and stakeholders a concrete basis for prioritizing work, selecting and configuring technologies, sequencing implementation phases, and measuring whether the resulting architecture fulfills defined business and risk-management objectives. Requirements also preserve traceability: each design decision and deployment activity can be linked back to an identified gap and an intended Zero Trust outcome. The Cloud Security Alliance describes planning as a process of defining scope, priorities, and a business case, supported by understanding the organization's existing environment and required future capabilities. NIST likewise frames Zero Trust planning around documenting the current state, desired state, and the changes needed to move between them. See the Cloud Security Alliance Zero Trust Planning guidance and NIST SP 800-207A.

QUESTION NO: 4

Network architects should consider_____ before selecting an SDP model.

Select the best answer.

A. leadership buy-in

B. gateways

C. their use case

D. cost

ANSWER: C

Explanation:

Network architects should consider **their use case** before selecting a Software-Defined Perimeter (SDP) deployment model. SDP is an architectural approach that establishes application-level, identity-aware connectivity only after authenticating and authorizing a requesting entity. The appropriate model depends on the organization's specific operational and security context rather than on a universal deployment preference. Relevant use-case factors include the resources requiring protection, where users and protected services are located, whether access is primarily for remote users, cloud workloads, or on-premises systems, and the organization's existing network topology. Architects must also account for expected scale, latency and performance needs, integration requirements, and the desired enforcement points for policy decisions. Assessing these factors enables the organization to select an SDP model that provides secure, least-privileged connectivity while fitting its environment and business objectives. CSA describes SDP deployment models as alternatives designed for differing application-access scenarios, making use-case analysis the essential selection criterion. See the Cloud Security Alliance SDP and Zero Trust guidance and CSA's overview of SDP deployment models.

QUESTION NO: 5

Which component in a ZTA is responsible for deciding whether to

grant access to a resource?

A. The policy enforcement point (PEP)

B. The policy administrator (PA)

C. The policy engine (PE)

D. The policy component

ANSWER: C

Explanation:

The policy engine (PE) is responsible for making the access decision in a zero trust architecture. It evaluates whether a subject should be granted access to a specific enterprise resource by applying organizational policy together with available contextual information. This decision can incorporate identity attributes, device security posture, requested resource characteristics, observed behavior, threat intelligence, and other information supplied by supporting policy-information sources. The policy engine's role is therefore evaluative and decisional: it determines whether the requested access should be authorized and can also determine conditions associated with that authorization. After reaching its decision, the policy engine communicates it to the policy administrator, which establishes or terminates the relevant connection, while the policy enforcement point enforces that connection at the resource boundary. This separation of decision, administration, and enforcement is fundamental to the NIST zero trust architecture model and enables access to be continually assessed rather than assumed based solely on network location. See NIST SP 800-207, section 3.3.1, Zero Trust Architecture, and the Cloud Security Alliance's Zero Trust Guidance.

QUESTION NO: 6

Scenario: As a ZTA security administrator, you aim to enforce the

principle of least privilege for private cloud network access. Which

ZTA policy entity is mainly responsible for crafting and maintaining

these policies?

A. Gateway enforcing access policies

B. Policy enforcement point (PEP)

C. Policy administrator (PA)

D. Policy decision point (PDP)

ANSWER: D

Explanation:

Policy decision point (PDP) is correct because it is the logical Zero Trust Architecture function responsible for evaluating access requests against policy and determining whether access should be granted. Least-privilege policy requires decisions to be based on the specific resource requested, the authenticated identity, device posture, environmental context, risk signals, and applicable organizational rules. By centrally applying and maintaining these decision criteria, the policy decision point ensures that authorization is narrowly scoped to the access needed for the requested action rather than relying on broad, persistent network trust.

In the NIST Zero Trust Architecture model, the policy decision point comprises the policy engine and policy administrator. The policy engine uses enterprise policy and inputs from supporting systems to make the allow, deny, or revoke decision, while the policy administrator translates that decision into instructions used to establish or terminate a session. Treating the combined decision function as the policy decision point is therefore appropriate when the question asks which policy entity is responsible for the policies governing least-privilege access. See NIST SP 800-207, Zero Trust Architecture and the Cloud Security Alliance Zero Trust Guidance for Enterprise.

QUESTION NO: 7

In a ZTA, the logical combination of both the policy engine (PE) and

policy administrator (PA) is called

A. policy decision point (PDP)

B. policy enforcement point (PEP)

C. data access policy

ANSWER: A

Explanation:

The correct term is **policy decision point (PDP)**. In the Zero Trust Architecture model defined by NIST, the PDP is the logical control-plane function that comprises the policy engine and the policy administrator. The policy engine evaluates access requests using enterprise policy together with relevant contextual inputs, such as identity, device posture, threat intelligence, and resource attributes. It then produces an allow, deny, or other access decision. The policy administrator takes that decision and carries out the associated operational action, such as establishing, modifying, or terminating the communication path between the requesting subject and the protected resource.

Describing these functions together as a PDP is important because it distinguishes the decision-making and session-management functions from enforcement. The PDP communicates its decision to an enforcement mechanism, while the PDP itself remains responsible for making policy-driven, context-aware authorization decisions. This separation supports Zero Trust's continuous evaluation approach: trust is not assumed from network location or granted permanently after initial authentication. NIST explicitly defines the PDP as the logical entity consisting of the policy engine and policy administrator in its Zero Trust Architecture guidance. See NIST SP 800-207, Zero Trust Architecture and the CISA Zero Trust Maturity Model.

QUESTION NO: 8

What should an organization ' s data and asset classification be based on?

A. Location of data

B. History of data

C. Sensitivity of data

D. Recovery of data

ANSWER: C

Explanation:

Data and asset classification should be based on the sensitivity of data. In a Zero Trust program, classification identifies the relative value of information and the degree of protection it requires against unauthorized access, disclosure, alteration, or loss. Sensitivity is determined by the potential business impact if the data is compromised, including effects on customers, operations, intellectual property, finances, and organizational reputation. Classification decisions also account for applicable legal, regulatory, privacy, and contractual requirements, because these obligations may mandate specific handling, retention, access-control, encryption, or breach-notification measures. Once sensitivity is established, the organization can consistently apply proportionate Zero Trust policies: least-privilege access, continuous authorization, data labeling, encryption, monitoring, and data-loss-prevention controls. NIST Zero Trust Architecture identifies data as an enterprise resource and explains that policies should protect resources regardless of their network location; understanding the resource's value and required protections is therefore central to policy enforcement. The Cloud Security Alliance similarly treats data protection as a core Zero Trust concern, with controls aligned to the sensitivity and criticality of business data. See NIST SP 800-207, Zero Trust Architecture and the Cloud Security Alliance Zero Trust Guidance for Data Security.